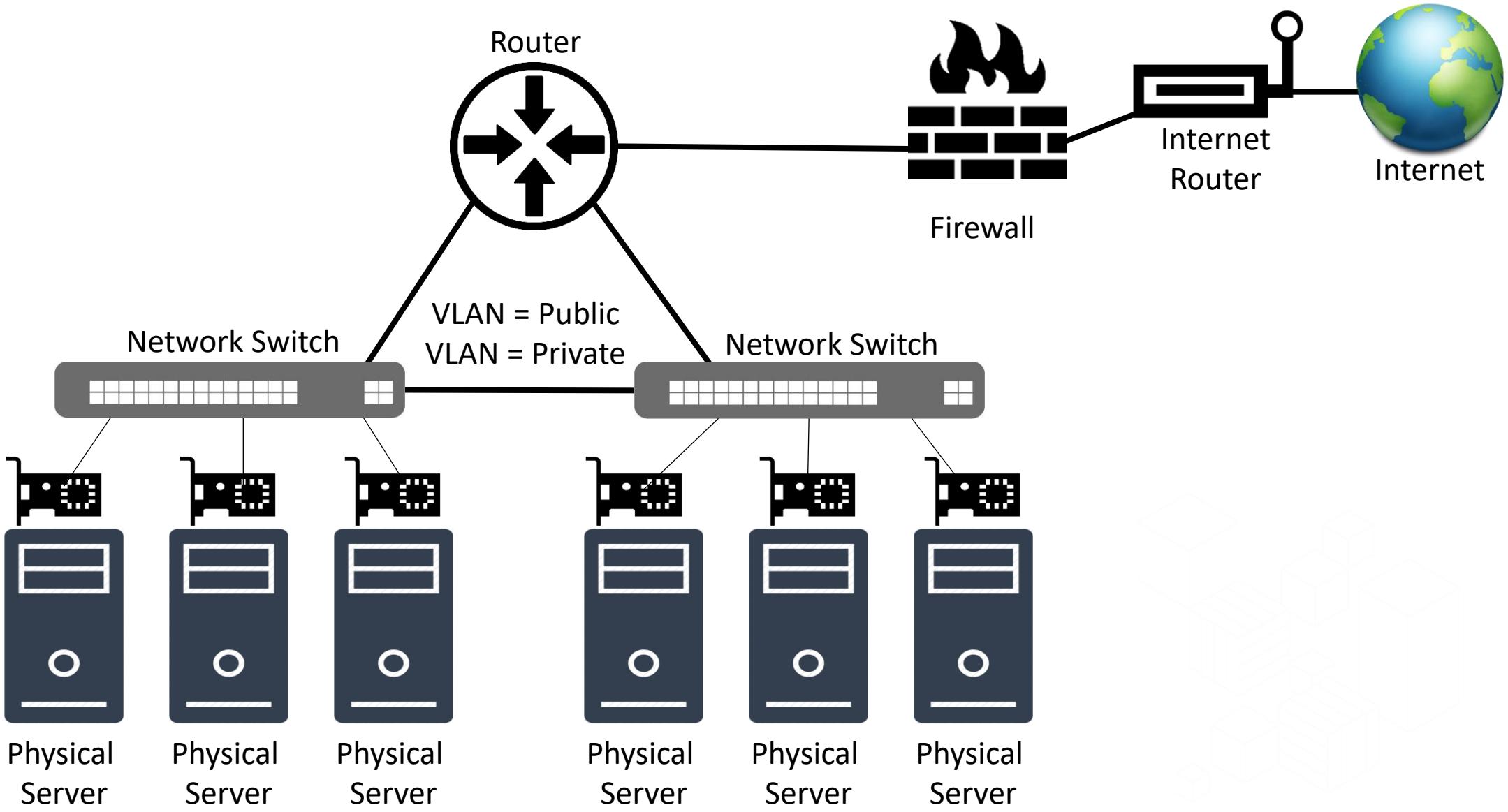
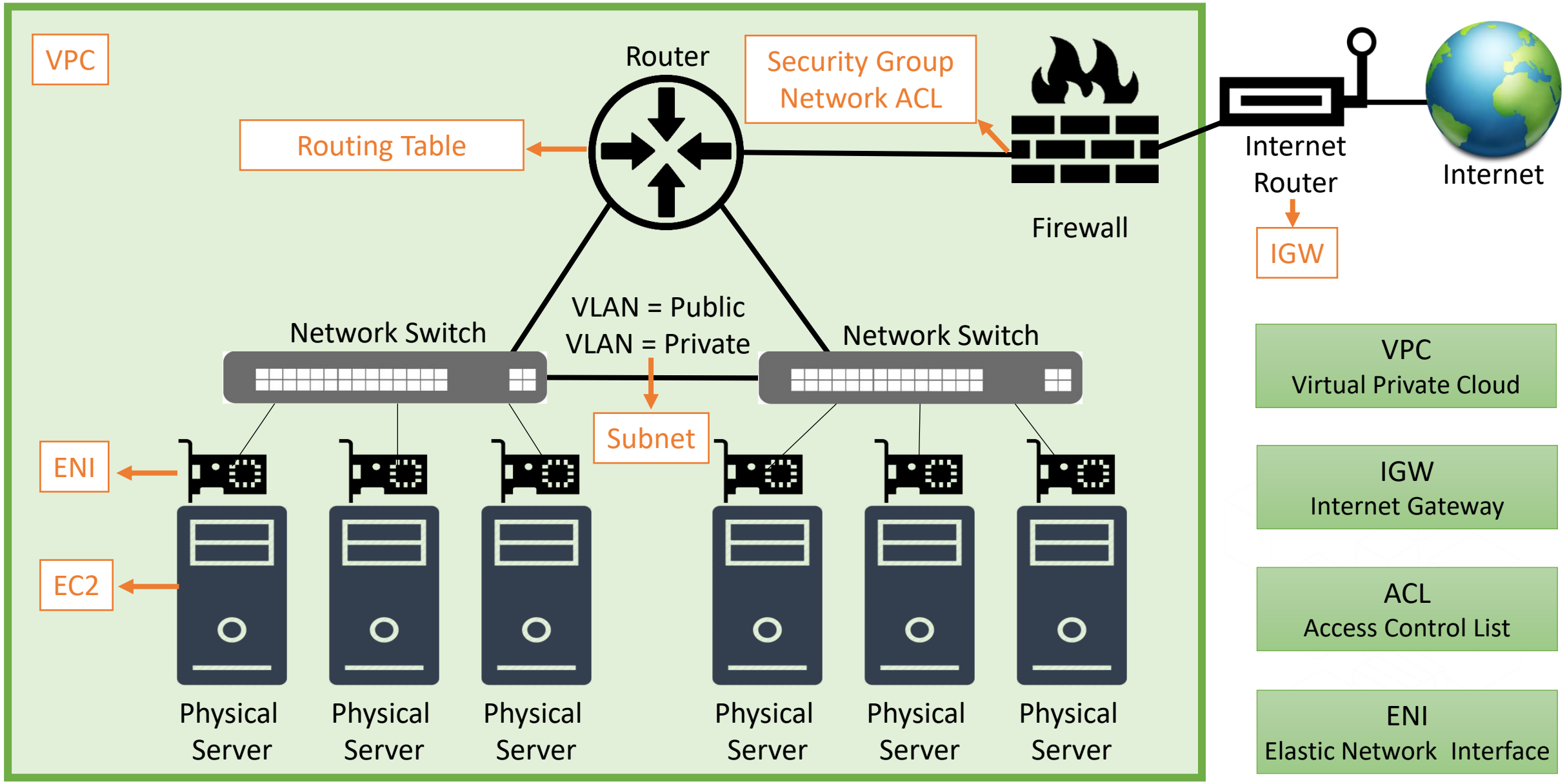
Networking in Cloud

Networking Basics

Networking in Physical World



Networking in AWS



VPC
Virtual Private Cloud

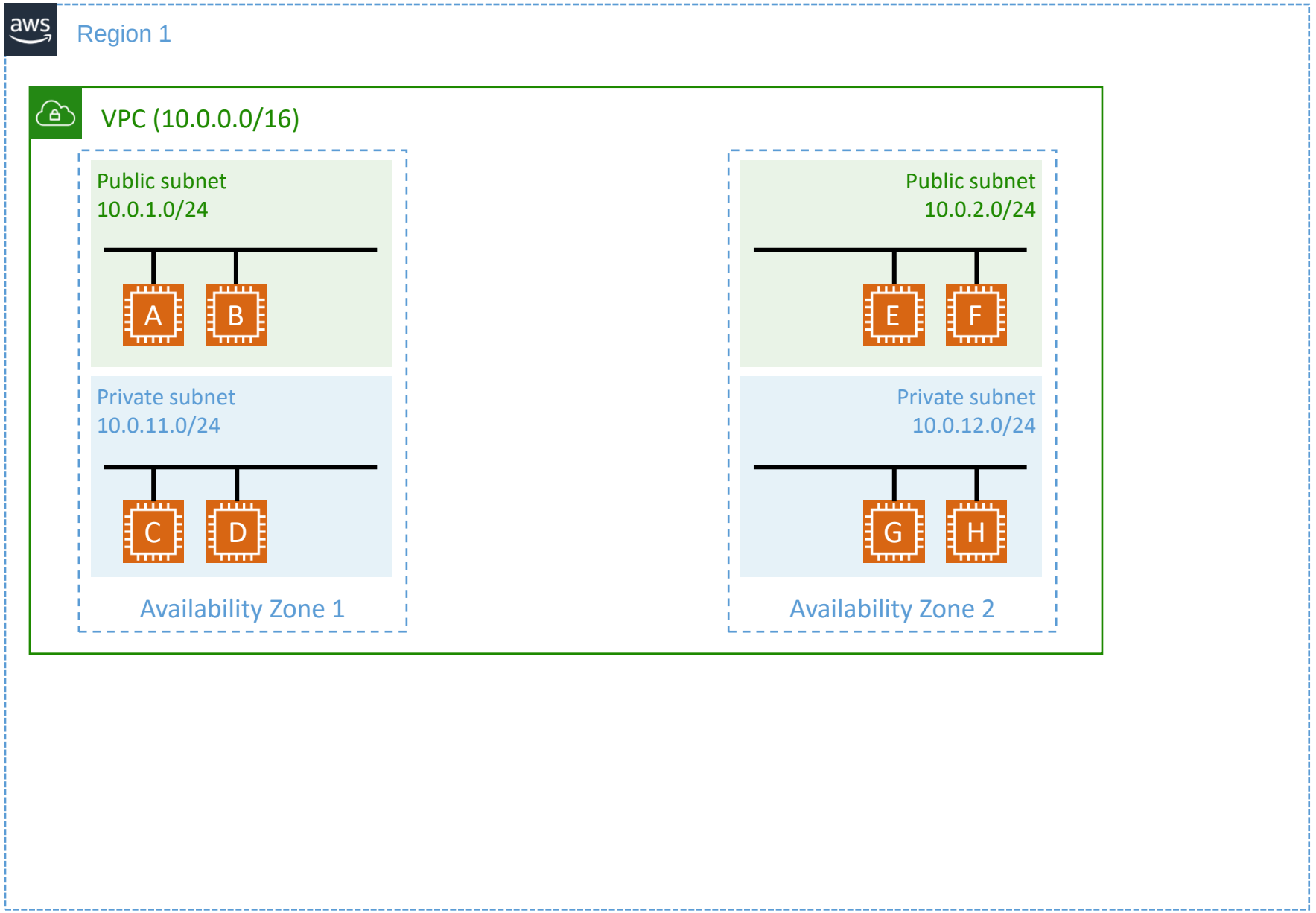
IGW
Internet Gateway

ACL
Access Control List

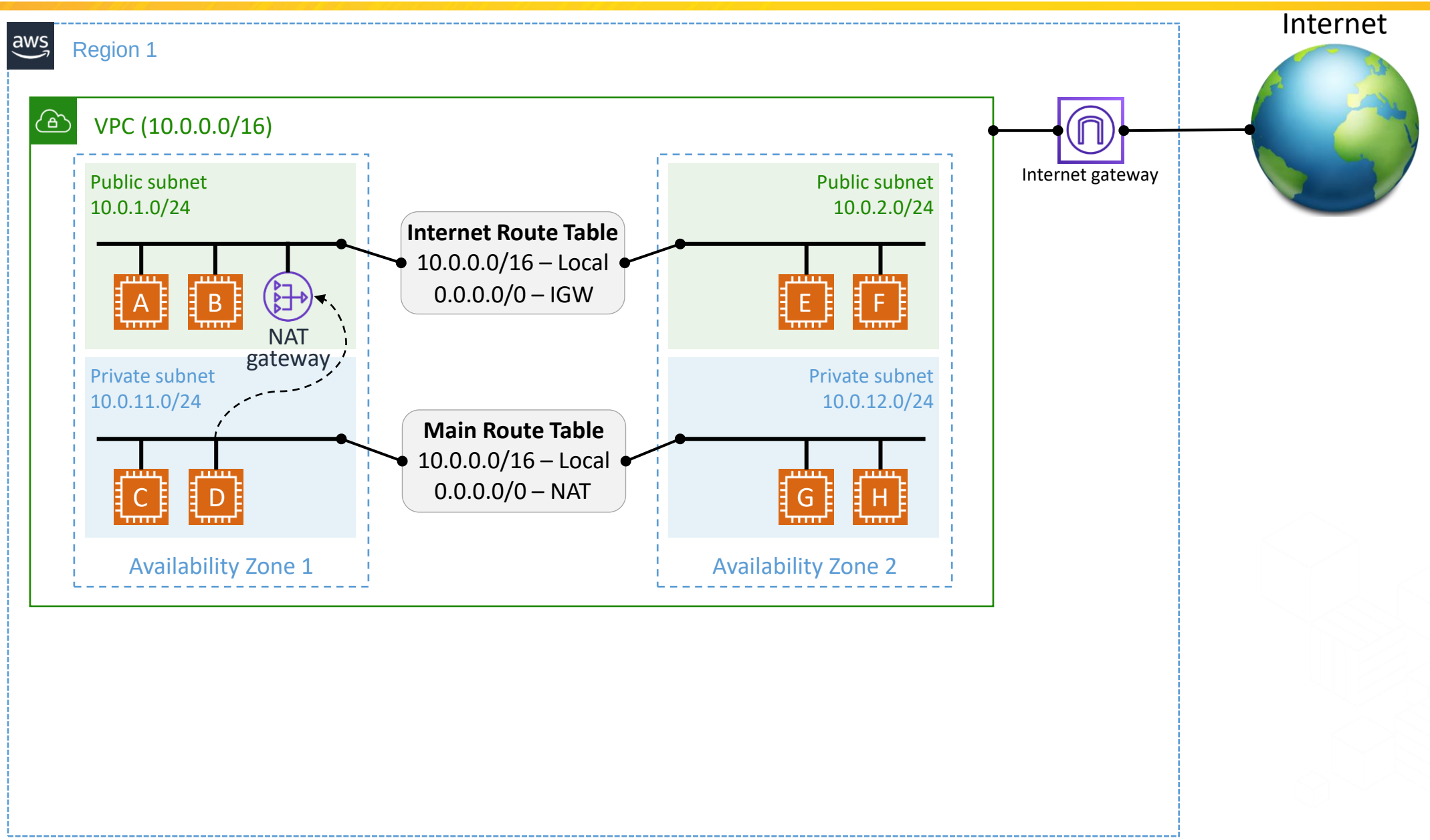
ENI
Elastic Network Interface

Amazon VPC

Amazon VPC

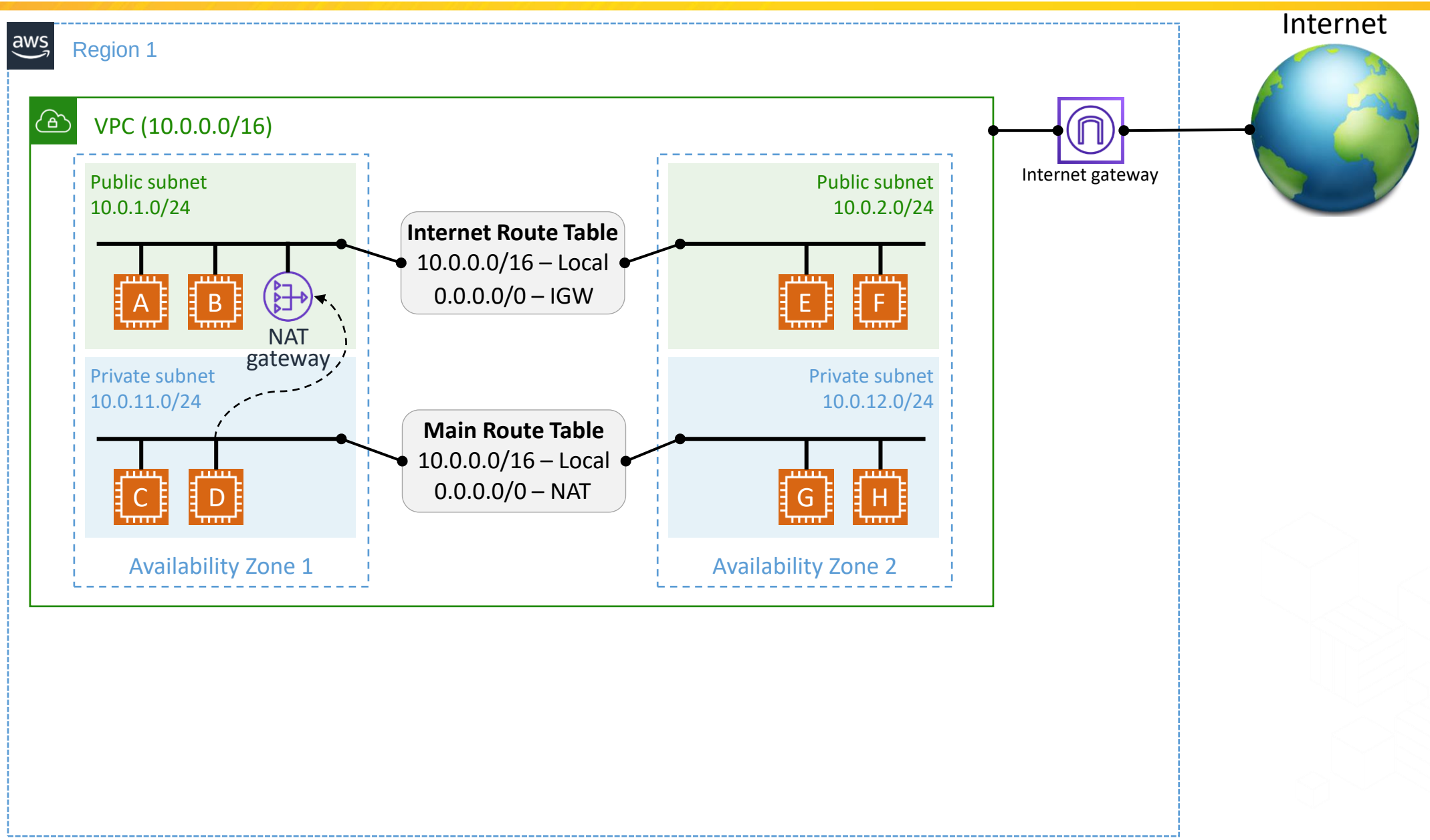

Region 1
VPC (10.0.0.0/16)
Public subnet
10.0.1.0/24
A
B
Private subnet
10.0.11.0/24
C
D
Availability Zone 1
Public subnet
10.0.2.0/24
E
F
Private subnet
10.0.12.0/24
G
H
Availability Zone 2

Amazon VPC

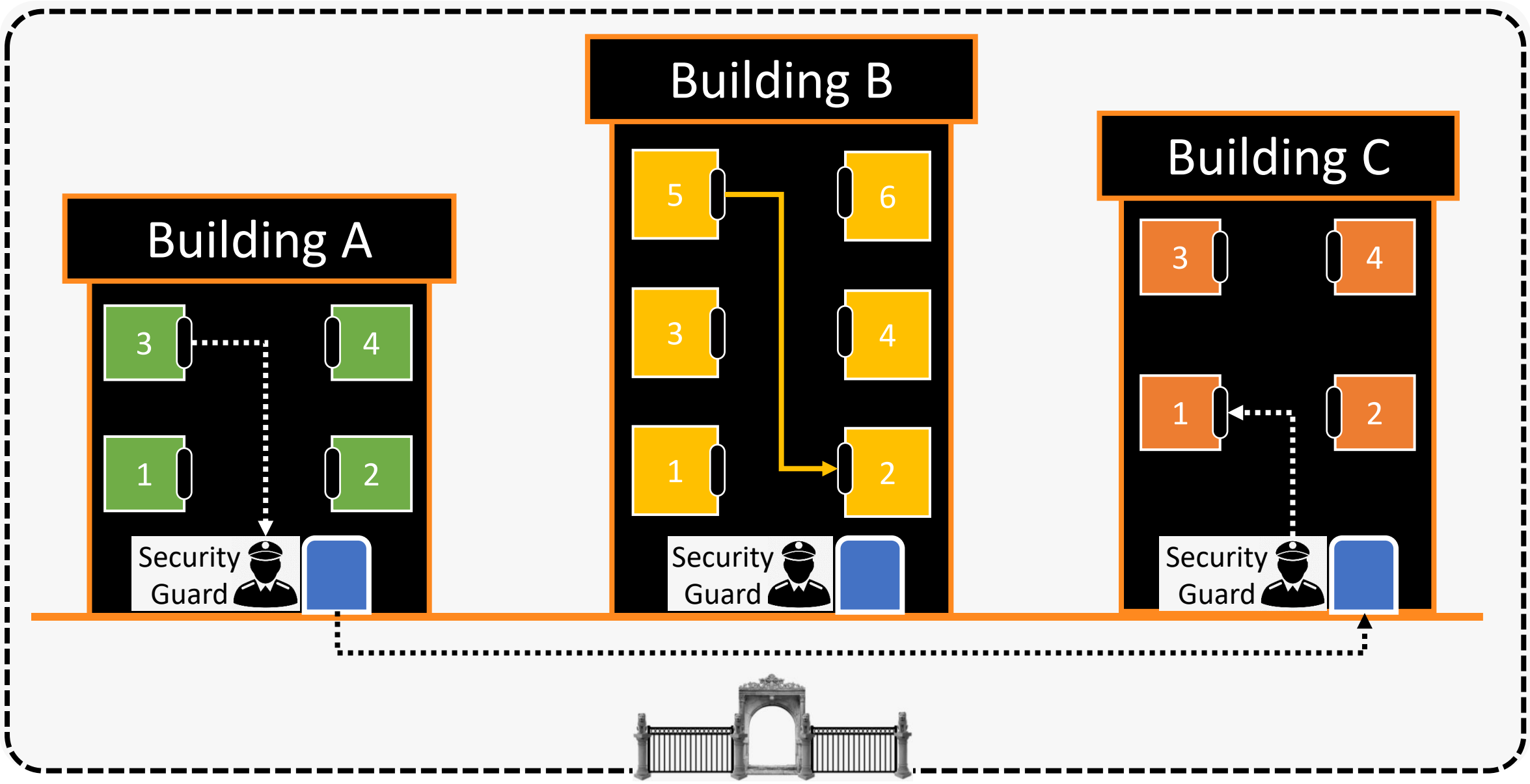

Region 1
VPC (10.0.0.0/16)
Public subnet
10.0.1.0/24
A
B
NAT gateway
Private subnet
10.0.11.0/24
C
D
Availability Zone 1
Internet Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – IGW
Main Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – NAT
Public subnet
10.0.2.0/24
E
F
Private subnet
10.0.12.0/24
G
H
Availability Zone 2
Internet gateway
Internet

Security Group
and
Network ACL

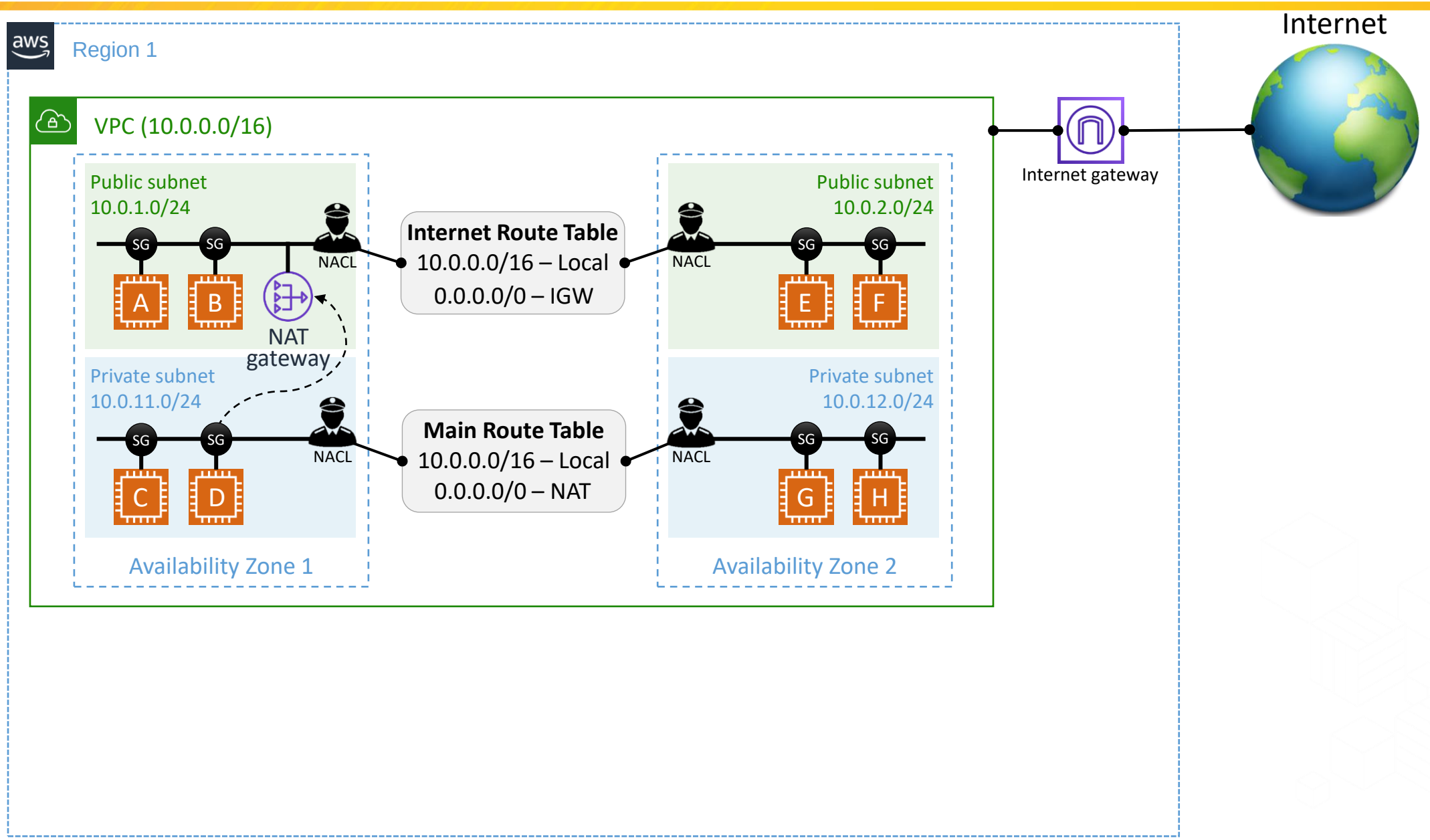
Amazon VPC


Region 1
VPC (10.0.0.0/16)
Public subnet
10.0.1.0/24
A
B
NAT gateway
Private subnet
10.0.11.0/24
C
D
Availability Zone 1
Internet Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – IGW
Main Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – NAT
Public subnet
10.0.2.0/24
E
F
Private subnet
10.0.12.0/24
G
H
Availability Zone 2
Internet gateway
Internet

Security Group and Network ACL



Amazon VPC


Region 1
VPC (10.0.0.0/16)
Public subnet
10.0.1.0/24
SG
SG
NACL
A
B
NAT gateway
Private subnet
10.0.11.0/24
SG
SG
NACL
C
D
Availability Zone 1
Internet Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – IGW
Main Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – NAT
Public subnet
10.0.2.0/24
NACL
SG
SG
E
F
Private subnet
10.0.12.0/24
NACL
SG
SG
G
H
Availability Zone 2
Internet gateway
Internet

Security Group vs. Network ACL

Security Group	Network ACL
Applied at Instance (ENI) Level	Applied at Subnet Level
Stateful - Response is always allowed	Stateless - Request and Response both have to be allowed

UK Immigration	India Immigration
	 
Stateful	**Stateless**

Security Group vs. Network ACL

Security Group	Network ACL
Applied at Instance (ENI) Level	Applied at Subnet Level
Stateful - Response is always allowed	Stateless - Request and Response both have to be allowed
Default Rules (For Default SG) - All inbound is allowed from the same SG - All outbound is Allowed Default Rules (For a new SG) - All Inbound is Deny - All outbound in Allowed	Default Rules (For Default NACL) - All inbound is Allowed - All outbound is Allowed Default Rules (For a new NACL) - All inbound is Deny - All outbound is Deny
1 Instance can have many SG assigned	1 Subnet can have only 1 NACL
Only allow statements	Allow and Deny both statements
Order is not important	Order is important (lower order rule is applied first)
Source - IP / IP Range / Port / SG-<xxxxxxx>	Source - IP / Port / IP Range

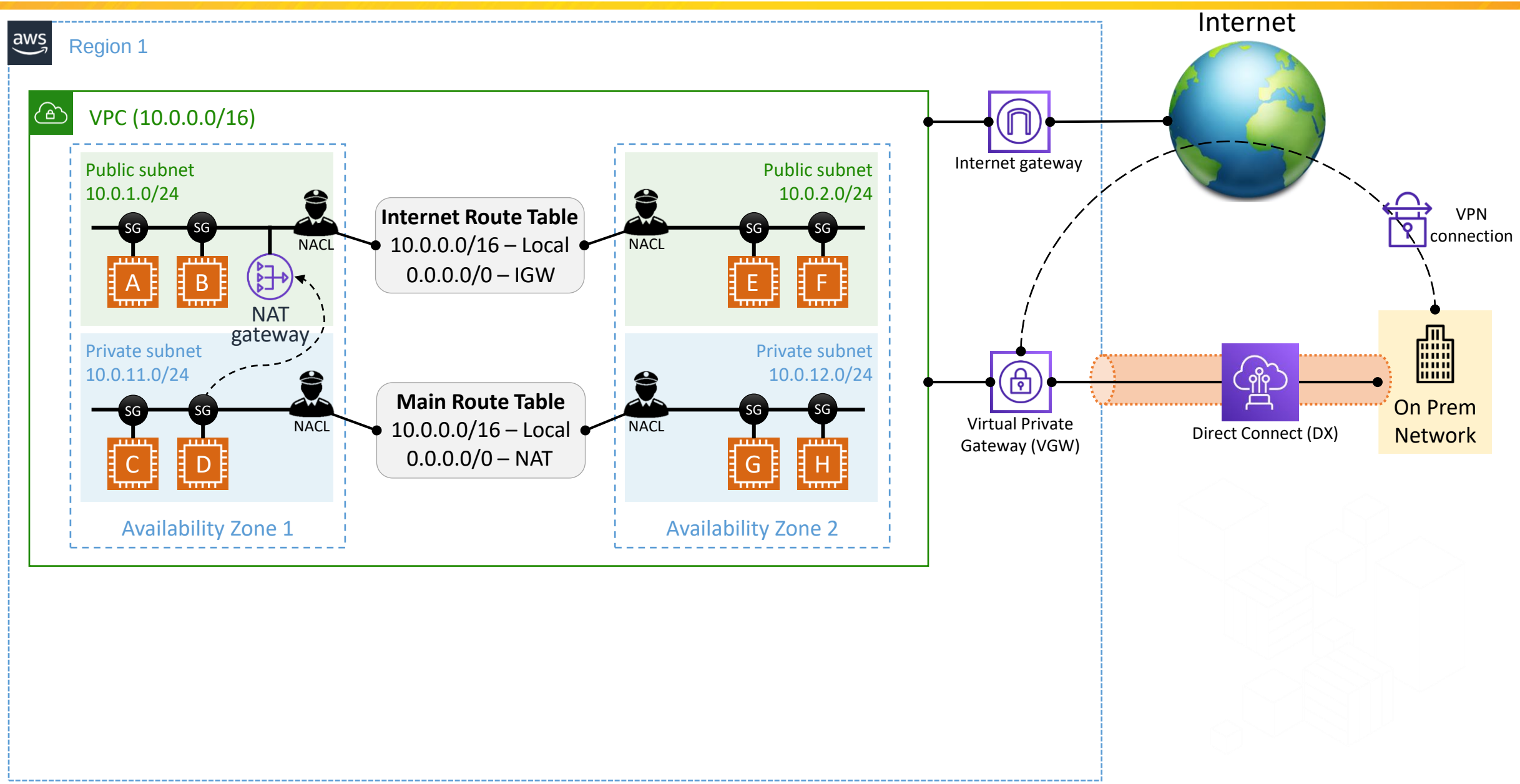
Private, Public and Elastic IP Addresses

Private, Public and Elastic IPs

	Private IP	Public IP	Elastic IP
Used for	Internal Communication	External Communication	External Communication
Mandatory / Optional	Mandatory	Optional	Optional
After Power Cycle	Stays same	Renewed	Stays same
Allocated to	Instance (ENI)	Instance (ENI)	Account (then associated)
Charges	No	No	Charged if unused

Site-to-Site VPN
and
Direct Connect

Amazon VPC


Region 1
VPC (10.0.0.0/16)
Public subnet
10.0.1.0/24
SG
SG
NACL
A
B
NAT gateway
Private subnet
10.0.11.0/24
SG
SG
NACL
C
D
Availability Zone 1
Internet Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – IGW
Main Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – NAT
Public subnet
10.0.2.0/24
NACL
SG
SG
E
F
Private subnet
10.0.12.0/24
NACL
SG
SG
G
H
Availability Zone 2
Internet gateway
Virtual Private Gateway (VGW)
Internet
VPN connection
Direct Connect (DX)
On Prem Network

Analogy - Site-to-Site VPN vs. Direct Connect

Commercial Flight

Site-to-Site VPN

Private Jet

Direct Connect

Site-to-Site VPN vs. Direct Connect

	Site-to-Site VPN	Direct Connect
Use case	Connecting remote networks to AWS VPC which doesn't require heavy data transfer or doesn't require a consistent connection	Connecting remote networks to AWS VPC which require heavy data transfer or require a consistent connection
Choose when…	Cost is important	Predictable performance is important
Supported speed	1.25 Gbps per tunnel	1 / 10 / 100 Gbps (sub 1 Gbps connections may be available from some service providers)
How it works?	Establishes a tunnel over existing internet connection	Establishes a connectivity over a dedicated network. Doesn't use Internet
High Availability	Highly available on AWS side (VGW is deployed across 2 AZs)	Single connection. No high availability by default
Encryption	Uses IPSec	Not encrypted by default
Time to establish	Can be setup in few minutes in a self-service fashion	Requires a Service Provider, may take few hours/days to get established
Cost dimension	Per connection hour and data transfer out	Variable port fees and data transfer out

Reference:

FAQs

Category:

Networking and Content Delivery

AWS Site-to-Site VPN

Complete book:

Click Here

Created by:

Ashish Prajapati

What?

- AWS Site-to-Site VPN creates a secure connection between your datacenter or branch office and your AWS cloud resources.
- Data transferred between your VPC and datacenter routes over an encrypted VPN connection using IPsec to help maintain the confidentiality and integrity of data in transit.

Why?

- With AWS Site-to-Site VPN you don't have to manage 3rd-party or custom VPN solutions built using EC2 instances.
- It has native integration with AWS Transit Gateway which allows customers to scale the connectivity to multiple VPCs with a single Transit Gateway-based VPN connection.

When?

- You want to extend your existing on-premises network into a VPC.
- You want to host Amazon VPCs behind your corporate firewall and seamlessly move your IT resources, without changing the way your users access these applications.

Where?

- AWS Site-to-Site VPN service is a regional service.
- It offers two VPN tunnels across multiple AZs, between a virtual private gateway or a transit gateway on the AWS side, and a customer gateway (which represents a physical device or software application) on the remote (on-premises) side.

Who?

- AWS Site-to-Site VPN is a fully-managed service.
- To enable instances in your VPC to reach your customer gateway, you must configure your route table to include the routes used by your Site-to-Site VPN connection and point them to your virtual private gateway or transit gateway.

How?

- You can create the Site-to-Site VPN connection using the customer gateway in combination with the virtual private gateway or transit gateway. After you create the Site-to-Site VPN connection, you can download a sample configuration file to use for configuring the customer gateway device.

How much?

- You are charged for each VPN connection hour that your VPN connection is provisioned and available. Each partial VPN connection-hour consumed is billed as a full hour.
- You also incur standard AWS data transfer charges for all data transferred via the VPN connection.

Reference:

FAQs

Category:

Networking and Content Delivery

AWS Direct Connect

Complete book:

Click Here

Created by:

Ashish Prajapati

What?

- AWS Direct Connect establishes a dedicated network connection between your on-premises network and AWS. With this connection in place, you can create virtual interfaces directly to the AWS Cloud, bypassing public internet.
- AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable.

Why?

- The AWS Direct Connect service is the shortest path to your AWS resources. While in transit, your network traffic remains on the AWS global network and never touches the public internet. This reduces the chance of hitting bottlenecks or unexpected increases in latency.

When?

- You want to build hybrid applications that span AWS and on-premises networks.
- You want to ensure smooth and reliable data transfers at massive scale for large datasets and need a predictable performance.

Where?

- AWS Direct Connect is a global service and available at locations worldwide.
- An AWS Direct Connect location provides access to AWS in the Region with which it is associated. You can use a single connection in a public Region to access public AWS services in all other public Regions.

Who?

- When creating a new connection, you can choose a dedicated connection from AWS (1 Gbps, 10 Gbps, or 100 Gbps) or hosted connection provided by an AWS Direct Connect Delivery Partner (50 Mbps up to 10 Gbps).

How?

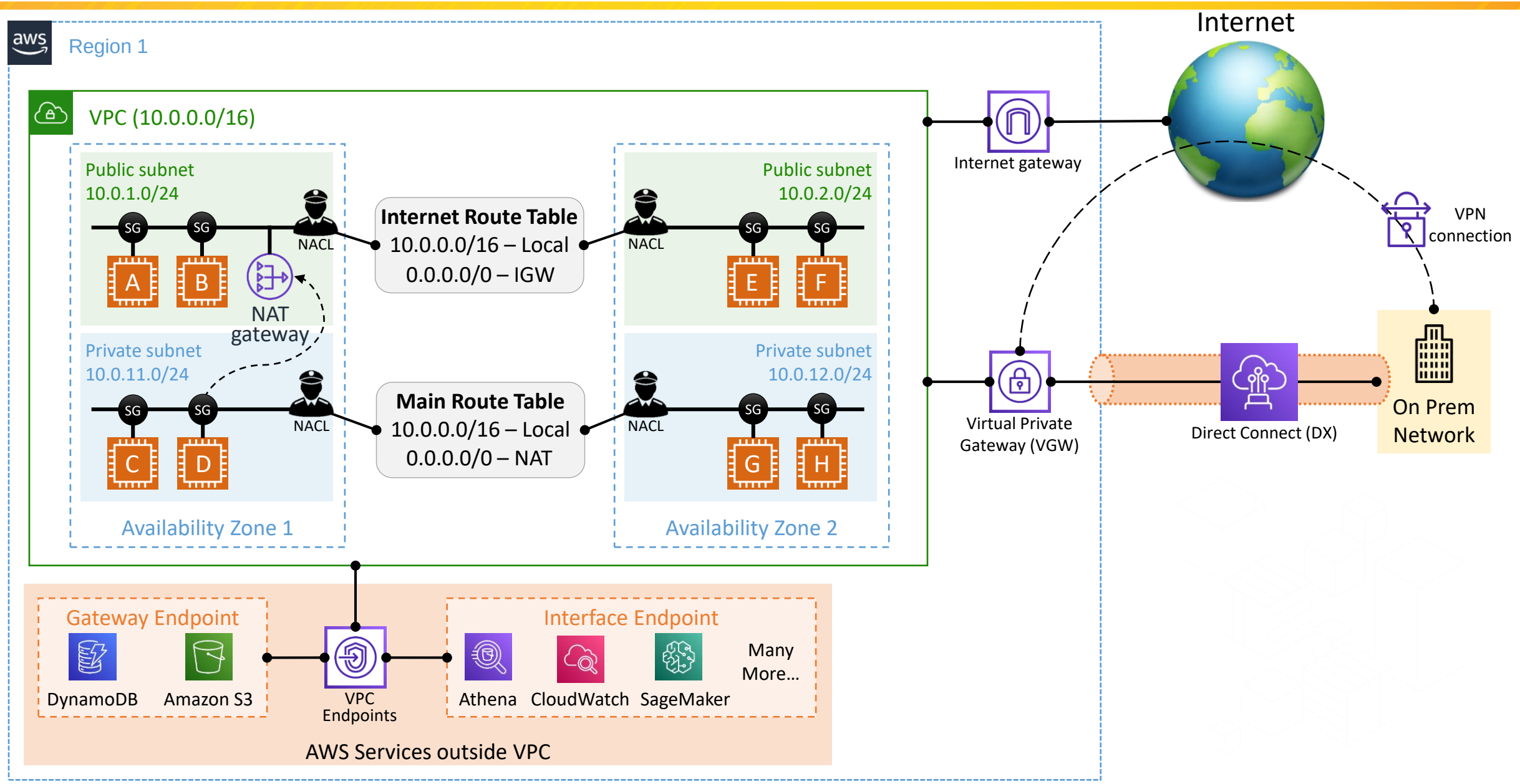
- After deciding on an AWS Direct Connect location and connection size, create your connection request on the AWS management console. Download Letter of Authorization (LoA) and provide it to an APN partner and ask them to establish the connection on your behalf.

How much?

- There are three factors that determine pricing: capacity (measured in Mbps Gbps), port hours (measure the time that a port is provisioned), and data transfer out (DTO) (charged per GB).
- AWS Direct Connect data transfer-in is free.

VPC Endpoints

Amazon VPC


Region 1
VPC (10.0.0.0/16)
Public subnet
10.0.1.0/24
SG
SG
NACL
A
B
NAT gateway
Private subnet
10.0.11.0/24
SG
SG
NACL
C
D
Availability Zone 1
Internet Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – IGW
Main Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – NAT
Public subnet
10.0.2.0/24
NACL
SG
SG
E
F
Private subnet
10.0.12.0/24
NACL
SG
SG
G
H
Availability Zone 2
Internet gateway
Internet
VPN connection
Virtual Private Gateway (VGW)
Direct Connect (DX)
On Prem Network
Gateway Endpoint
DynamoDB
Amazon S3
VPC Endpoints
Interface Endpoint
Athena
CloudWatch
SageMaker
Many More...
AWS Services outside VPC

VPC Endpoints

	Gateway Endpoint	Interface Endpoint
Used for	Private connectivity to Amazon S3 and Amazon DynamoDB	Private connectivity to 100+ AWS Services (including Amazon S3)
How it works?	An entry for prefix list (IP addresses) for supported services is added in to the routing table	An ENI(s) is provisioned in the selected subnet(s) which serves as an entry point for traffic destined to a supported service. (powered by AWS PrivateLink)
Provisioned at	VPC Level then entry added to Route Table	Subnet Level (no entry required in Route Table)
Security	Through VPC Endpoint Policy	Through Security Group

Reference:

FAQs

Category:

Networking and Content Delivery

AWS PrivateLink

Complete book:

Click Here

Created by:

Ashish Prajapati

What?

- AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet.
- You can host your own AWS PrivateLink powered service, known as an *endpoint service*, and share it with other AWS customers.

Why?

- Network traffic that uses AWS PrivateLink doesn't traverse the public internet, reducing exposure to brute force and distributed denial-of-service attacks, along with other threats.

When?

- You want to use services offered by another VPC securely within the AWS network, without all network traffic staying on the global AWS backbone and never traversing the public internet.

Where?

- The interface endpoints are created directly inside of your VPC, using elastic network interfaces and IP addresses in your VPC's subnets.

Who?

- As a service user, you will need to create interface type VPC endpoints for services that are powered by PrivateLink.
- As a service owner, you can onboard your service to AWS PrivateLink by establishing a Network Load Balancer (NLB) to front your service and create a PrivateLink service to register with the NLB.

How?

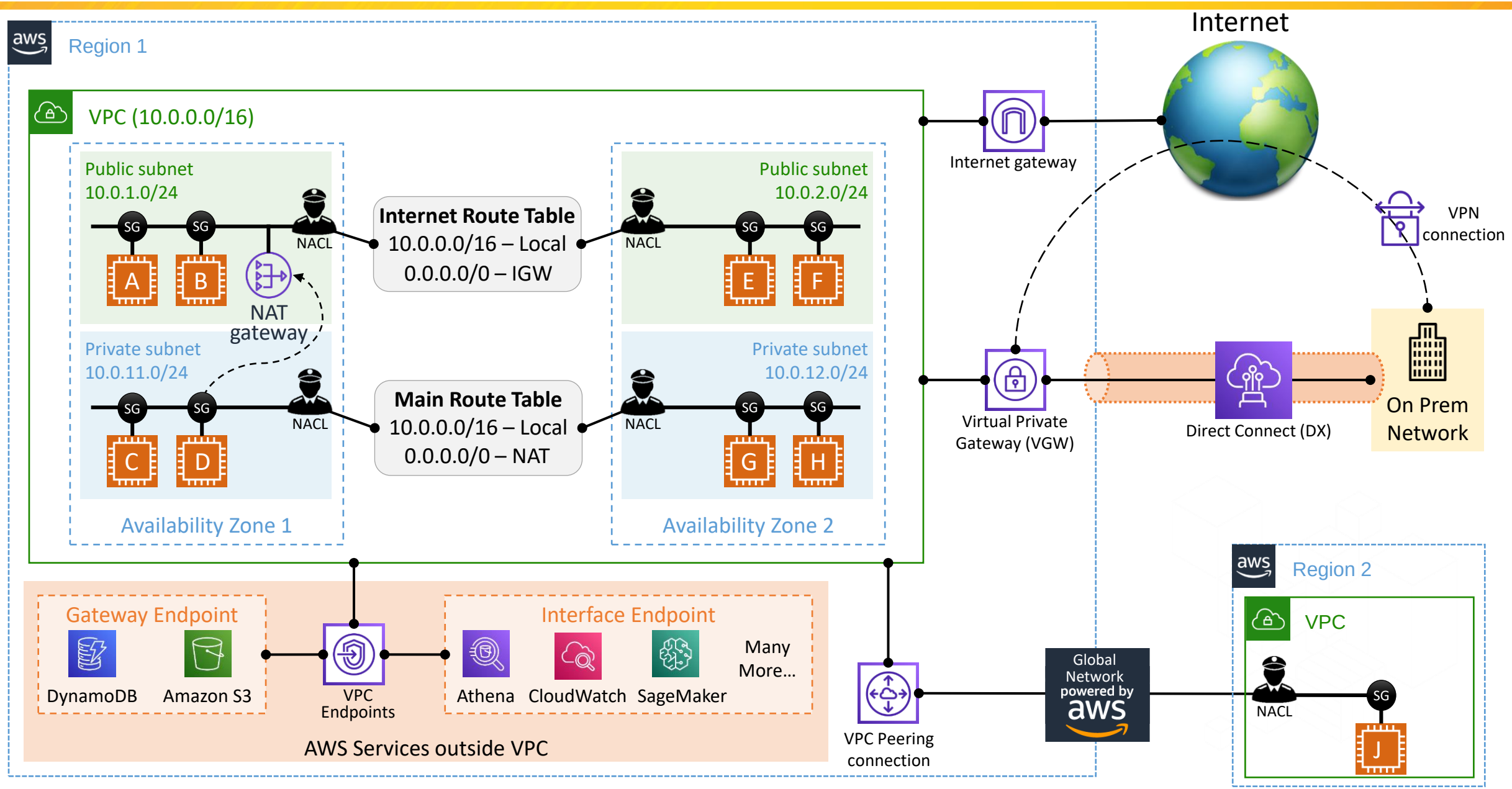
- To use AWS PrivateLink, create an interface VPC endpoint for a service outside of your VPC. This creates an elastic network interface in your subnet with a private IP address that serves as an entry point for traffic destined to the service.

How much?

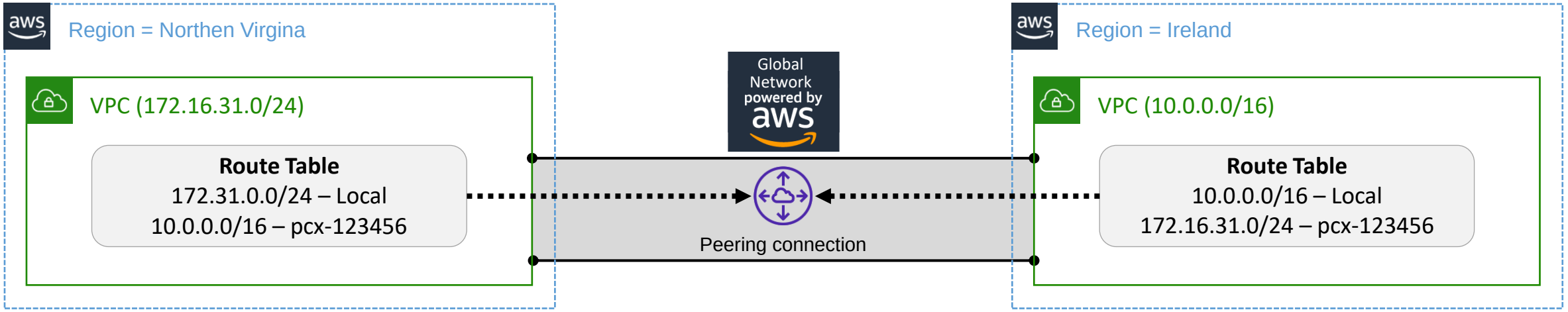
- You are charged for each hour that your VPC endpoint is provisioned in each Availability Zone.
- Data processing charges apply for each Gigabyte processed through the VPC endpoint regardless of the traffic's source or destination.

VPC Peering

Amazon VPC Peering



VPC Peering



- VPC Peering is established in a 1:1 fashion and is not transitive.
- You can setup cross-region, cross-account peering.
- Two step process – Request Peering and Accept Peering.
- Route Table entries direct the traffic.
- Peering connection uses private IP Address, traffic always stays on the global AWS backbone.
- There is no charge to create a VPC peering connection but there is a charge for data transfer across peering connections.

Reference:

FAQs

Category:

Networking and Content Delivery

Amazon VPC

What?

- Amazon Virtual Private Cloud (Amazon VPC) enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you have defined.
- This virtual network closely resembles a traditional network that you would operate in your own data center.

Why?

- You can define your own network space, and control how your network and the Amazon EC2 resources inside your network are exposed to the Internet.
- You can also leverage more granular access to and from the Amazon EC2 instances in your virtual network.

When?

- You want to launch AWS resources in a logically isolated virtual network and spend less time setting up, managing, and validating your virtual network.
- You want to use multiple layers of security, including security groups and network access control lists.

Where?

- VPC is a regional entity and spans across all of the Availability Zones in the region.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.
- You can launch AWS resources, such as EC2 instances, into a specific subnet.

Who?

- Your AWS resources are automatically provisioned in a ready-to-use default VPC or you can create additional VPCs.
- You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.

How?

- When you create a VPC, you must specify an IPv4 CIDR block for the VPC. Afterwards you can add subnets, route tables, security groups, network access control list, an internet gateway, and other gateways as necessary.

Created by:

Ashish Prajapati

How much?

- There is no additional charge for using a VPC. There are charges for some VPC components, such as NAT gateways, Reachability Analyzer, and traffic mirroring. Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources, including data transfer charges.